AMENDMENTS TO THE SPECIFICATION

In the Specification:

Please make the changes specified below to the paragraphs at page 13, line 16 to page 14, line 18:

If the security analyzer 730 determines a suitable security level for the remote device 710, then one or more access keys 740 can be transferred to the automation component 720 to control network access thereto. The access keys 740 may contain attribute information to enable one or more access controls 744 to operate an associated security switch 750. When enabled, the security switch 750 allows or controls communications between the automation component 720 and the remote device [[720]]710. In one example, the access keys 740 (*e.g.,* digital codes describing how, who, when, where, and under what circumstances access is to be granted) may include time and/or location information to control access of the remote device 710. For example, the access keys 740 may stipulate that the remote device [[700]]710 is to be granted network access for 10 minutes, only from network requests originating from Chicago, from either business managers or maintenance personnel, data can only be read from the automation component, and have an associated authentication/authorization key or code to verify that the remote device is the machine that originally negotiated with the security analyzer 730. Given that time coded information can be contained within the access keys 740, the access controls 744 can be timed and/or checked after the time specified in the access keys has expired, wherein the security switch 750 is then disabled to outside network communications from the remote device [[720]]710.

It is to be appreciated that a plurality of security and/or attribute information can be contained within the access keys 740 to subsequently control the security switch 750. For example batch, process, program, calendar, GPS (Global Positioning Information) to specify local and/or wireless network locations, memory restrictions (*e.g.,* can access I/O memory but not program memory), and other information or security attributes may be included as part of the access keys 740 to control access to the automation component 720. In one example, the access keys 740 may specify that during real time batch processing, no access may be granted to the

automation component 720, otherwise, during other program or automated operations, no such network restriction is required. As noted above, the security computer 724 and/or analyzer 730 can continue to monitor network traffic. If a security problem is detected, the security computer 740 can issue new access keys 740 (or alter previous keys) that revoke and/or limit the network access of the remote device [[720]]710.